

WHAT IS CLAIMED IS:

- 1 1. A machine-implemented method comprising:
2 producing a first authentication message comprising:
3 authentication data encrypted with a first key; and
4 a data structure comprising the first key, wherein
5 the data structure is encrypted with a second key;
6 generating a request message to have a first network
7 device associated with a first network deliver datagrams
8 destined for a home address associated with a mobile device on
9 the first network to a second address on a second, different
10 network; and
11 embedding the authentication message in the request
12 message.
- 1 2. The method of claim 1 wherein the authentication data
2 comprises a timestamp.
- 1 3. The method of claim 1 wherein the second key is known to
2 the first network device and unknown to the mobile node.
- 1 4. The method of claim 1 wherein the authentication message
2 comprises a Kerberos Application Request.
- 1 5. The method of claim 1 wherein the data structure
2 comprises a Kerberos ticket.

1 6. The method of claim 1 further comprising generating a
2 second authentication message.

1 7. The method of claim 6, wherein generating a second
2 authentication message comprises:
3 generating a hash of the request message using the first
4 key.

1 8. The method of claim 6 further comprising:
2 transmitting the request message and second
3 authentication message to the first network device.

1 9. The method of claim 8 further comprising:
2 receiving the request message and second authentication
3 message by a device on the home network; and
4 decrypting the data structure using the second key to
5 obtain the first key.

1 10. The method of claim 9 further comprising:
2 verifying the second authentication message using the
3 first key.

1 11. The method of claim 9 further comprising generating a
2 third key.

1 12. The method of claim 9 further comprising generating
2 key material, wherein the key material may be supplied to a
3 function to generate a third key.

1 13. The method of claim 1 wherein the request message
2 comprises a Registration Request message.

1 14. The method of claim 11 further comprising:
2 forming a reply authentication message comprising the
3 third key encrypted with the first key.

1 15. The method of claim 14 wherein the reply authentication
2 message comprises a Kerberos Application Reply message.

1 16. The method of claim 14 further comprising:
2 forming a reply message that includes the reply
3 authentication message.

1 17. The method of claim 16 wherein the reply message
2 comprises a Registration Reply message.

1 18. The method of claim 16 further comprising:
2 generating a third authentication message; and
3 transmitting the reply message and third authentication
4 message to the mobile node.

1 19. The method of claim 18 wherein generating a third
2 authentication message comprises:

3 generating a hash of the reply authentication message
4 using the first key.

1 20. A machine-implemented method comprising:

2 receiving at a first device associated with a home
3 network an authentication message and a request message to
4 reroute datagrams destined for a first address of a mobile
5 device associated with the home network to a second address
6 not associated with the home network, wherein the request
7 message comprises:

8 a data structure that includes a first key encrypted
9 with a second key; and

10 determining if the authentication message is valid.

1 21. The method of claim 20 further comprising:

2 generating a third key if the authentication message is
3 determined to be valid.

1 22. The method of claim 20 further comprising:

2 generating key material if the authentication message is
3 determined to be valid, wherein the key material may be

4 supplied to a function known to the first device and the
5 mobile device to produce a third key.

1 23. The method of claim 20 wherein the authentication message
2 comprises a hash of the request message, wherein the hash is
3 computed using the first key.

1 24. The method of claim 20 wherein the request message
2 comprises a Registration Request message.

1 25. The method of claim 23, wherein determining if the
2 authentication message is valid comprises:
3 computing a hash of the request message using the first
4 key; and
5 comparing the computed hash to the authentication
6 message.

1 26. The method of claim 25 further comprising:
2 decrypting the data structure using the second key to
3 obtain the first key.

1 27. The method of claim 21 further comprising:
2 receiving a reply message from the first device by the
3 mobile device, wherein the reply message includes the third
4 key.

28. The method of claim 27 further comprising:

forming a second request message to have datagrams destined for a first address of a mobile device associated with the home network to a third address not associated with the home network;

forming a second authentication message using the third key; and

transmitting the second request message and second authentication message to the first device.

29. A computer program product residing on a computer readable medium having instructions stored thereon that, when executed by the processor, cause that processor to:

form an authentication message comprising:

authentication data encrypted with a first key; and

the first key encrypted with a second key;

generate a request message requesting that datagrams destined for a first Internet Protocol address of a mobile device be routed to a second Internet Protocol address; and

include the authentication request message in the request message.

1 30. The computer program product of claim 29 wherein the
2 authentication message comprises a Kerberos Application
3 Request message.

1 31. The computer program product of claim 29 further
2 comprising instructions to generate a hash of the request
3 message using the first key to form a second authentication
4 message.

1 32. The computer program product of claim 29 further
2 comprising instructions to:

3 receive a reply message from the first device by the
4 mobile device, wherein the reply message includes a third key;
5 form a second authentication message using the third key;
6 transmit a second request message to have datagrams
7 destined for a first address of a mobile device associated
8 with the home network to a third address not associated with
9 the home network, wherein the second authentication message is
10 included in the second request message.

1 33. A computer program product residing on a computer
2 readable medium having instructions stored thereon that, when
3 executed by the processor, cause that processor to:

4 extract an authentication message from a message
5 requesting that datagrams destined for a first Internet
6 Protocol address of a mobile device be routed to a second
7 Internet Protocol address, wherein the authentication message
8 comprises:

9 authentication data encrypted with a first key; and
10 a data structure comprising the first key, and
11 encrypted with a second key;

12 verify the authentication data; and

13 if the authentication data is valid, then generating a
14 third key.

1 34. The computer program product of claim 33 further
2 comprising instructions that cause the processor to:

3 form a reply message that includes the third key; and
4 transmit the reply message to a device associated with
5 the request message.

1 35. The computer program product of claim 33 further
2 comprising instructions that cause the processor to:

3 store the encryption key.

1 36. The computer program product of claim 33 wherein the
2 message comprises a Registration Request message.

1 37. A system comprising:

2 a first network device associated with a first network;

3 and

4 a second network device associated with the first
5 network, the second network device capable of:

6 producing an authentication message including a data
7 structure comprising the first key with the data structure
8 encrypted with a second key;

9 generating a request message to have the first network
10 device deliver datagrams destined for a home address
11 associated with the second device on the first network to a
12 second address on a second, different network; and

13 including the authentication message within the request
14 message.

1 38. The system of claim 37 wherein the second network device
2 is further capable of forming a second authentication message
3 by computing a hash of the request message using the first
4 key.

1 39. The system of claim 38 wherein the first network device
2 is capable of receiving the request message and generating a
3 key if the second authentication message is valid.

1 40. The system of claim 37 wherein the first network device
2 is a router.

1 41. The system of claim 37 wherein the second network device
2 is a laptop computer.

1 42. The system of claim 37 further comprising:
2 a third device capable of producing the first key and the
3 data structure encrypted with the second key.

1 43. A system comprising:
2 a router associated with a first network and comprising
3 an input port for receiving datagrams and a switch fabric for
4 determining destination of datagrams; and
5 a processor capable of:
6 reading request message to reroute datagrams
7 destined for a first address of a mobile device associated
8 with the first network to a second address associated with a
9 second, different network, wherein the request message
10 includes a data structure comprising a first key unknown to
11 the processor encrypted with a second key that is known to the
12 processor,
13 verifying an authentication message associated with
14 the request message wherein the authentication message

15 comprises a hashed version of the request message computed
16 using the first key; and
17 if the authentication message is valid, then generating a
18 third key.

1 44. The system of claim 43, wherein the processor is further
2 capable of:
3 encrypting the third key.

1 45. The system of claim 44, wherein the processor is further
2 capable of:
3 forming a reply message, wherein the reply message
4 includes the encrypted third key; and
5 forming a reply authentication message.

1 46 The method of claim 45 wherein the reply authentication
2 message comprises a hashed version of the reply message.

1 47. The method of claim 45 further comprising: transmitting
2 the reply message and the reply authentication message to the
3 mobile device at the second address.